Outsourcing Physician HIT Functions: How to Play with Application Services Provides ("ASPs") Without Being Bitten

American Health Lawyers Association
Physicians and Physician Organizations Law Institute
April 19 – 21, 2001

Author: John R. Christiansen, J.D.
Phone: 206.386.7520
jrchristiansen@stoel.com
STOEL RIVES LLP
600 University Street, Suite 3600
Seattle, Washington 98101-3197
Fax: 206.386.7500

1. Introduction

Healthcare information technology (collectively "HIT") has become a crucial part of the health care infrastructure. The integration of HIT is most advanced in the larger hospitals and health systems, but many physician practices have also adopted HIT in some form. This trend is only likely to accelerate as physician business partners such as hospitals and health plans require or create incentives for electronic interaction with physicians, leading practices raise the bar on physician HIT use, and HIT becomes less expensive to acquire.

Physician HIT is becoming more accessible in substantial part because of the rise of the business model of the "application services provider," or "ASP." An ASP may be defined as an independent provider of enterprise computer services to organizations, including network services, over the Internet or other network system, on a leased or subscription basis. An ASP funds its own acquisition of the data centers and connectivity necessary to provide its services, using invested capital and its own revenues.

Acquisition costs are recovered through network lease or subscription charges, spread across all ASP customers.

For good or bad, HIT is transforming the practice of medicine. Internet e-mail and website technologies are changing the ways physicians and patients communicate; on-line journals, CMEs and "evidence-based medicine" initiatives are beginning to affect standards of care; and health plans, hospitals and governmental healthcare agencies are implementing and requiring the physicians with which they do business to adapt to networks for the electronic exchange of clinical, claims and administrative information. Meanwhile new legal requirements for the protection of patient information, with unprecedented penalties for their violation, will become effective in the near future.

Some of these trends are pushed by legal mandates. In particular, the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") requires the standardized electronic data processing of claims transactions, and will establish national standards for the privacy and security of health care information. But there are social and market forces at work too. Patients have begun to use the Internet and other information resources to become more aggressive participants in their own care, and the competent use of technologies which fit a practice's real needs can greatly enhance the quality of the care delivered while helping manage costs.

But what HIT do physicians "really need," and how can they get them in a cost-effective, reliable fashion ? The former question has some answers that apply to almost all practices, but can only really be answered by the physicians themselves. The second question may in many cases best be answered by outsourcing information

applications to ASPs, so long as there are adequate assurances that these companies are themselves competent and reliable.

2. What Technologies Do Physicians Need?

Any technology, no matter how ultimately beneficial, comes at a cost, not all of which is obvious. The purchase prices for hardware or software, or subscription fee for an on-line service is easy to spot. The hidden costs of re-engineering practice methods to actually get the benefits of technology may not be so obvious. But both need to be taken into account in making the cost/benefit analysis which should guide any technology acquisition.

The specific cost/benefit analysis for any technology will depend upon the goals and needs of the practice. However, it is possible to give a short, general summary for the following major types of information technology which might be valuable to physicians:

Electronic Claims Processing. Electronic claims processing is likely to be a virtual "no-brainer" for any practice. HIPAA includes a legal mandate to all health plans to adopt standardized formats and process almost all claims transactions electronically. This mandate gives plans a strong incentive to insist that all providers they do business with submit and receive claims information electronically. Those practices which do not yet use electronic claims processing must expect strong, possibly irresistible pressures to do so over the next two years.

On the negative side, adoption of electronic claims processing will subject a practice to HIPAA's privacy and security requirements. This will require substantial examination of and probably some change to existing business practices. On the positive side, many health plans are developing systems which may allow much faster payment turnaround for electronic submissions.

On-line Journals and CMEs. On-line journals, CMEs and other medical information resources are another "no-brainer." Many medical journals now put most of their contents on-line where they are available for free, or for a reasonable subscription fee, and services like Medscape even provide free subscriptions to e-mail newsletters with journal updates. Unlike a traditional library, on-line resources are always open, and accessible from the office or home. And many organizations are offering on-line CMEs which, again, are accessible during off-hours from convenient locations, for practitioners whose schedules or locations make it hard to get to "in person" events.

Any practitioner who has a personal computer and Internet services subscription can access such services. It does take a little time to learn where resources are, but the added convenience should quickly outweigh this burden. And over time access to computer-based and on-line clinical information resources will become part of the standard of care for medical practice, making their use essential.

Web Sites. Setting up a website has become cheap and relatively easy. Websites may serve useful marketing or educational functions, and sometimes include functions such as scheduling which are of administrative value to both patient and physicians. Some organizations are exploring the use of "chat rooms" for patients,

sometimes including on-line "communities" and "chat" access to healthcare professionals Despite their potential value none of these functions is without some potential for risk.

One risk could be unexpected exposure to the laws of jurisdictions outside the state(s) where the organization is physically located. Websites by their nature communicate across jurisdictional boundaries, so if they include functions which could be deemed "doing business" they may subject the organization to other states' jurisdictions. (The same consideration may apply to activities involving mulit-jurisdictional information networks and telemedicine.) Under current mainstream law – to the extent there is "mainstream" law in this area - relatively passive, informational websites should not trigger jurisdictional concerns, but interactive website functions should be reviewed in this light before being implemented.

Many, perhaps most websites collect information about visitors, sometimes in considerable detail. The scope of acceptable information collection and the kinds of notices which may be required are topics of some controversy, and in some areas self-regulation "better business practices" are being developed. There have already been lawsuits filed when web sites failed to accurately disclose their information collection practices, and it is possible federal or state regulations will be implemented at some point.

There are also risks in the publication of information by websites. The most basic healthcare organization websites publish little more than basic information about facility locations, services and possibly health plan participation and some professional staff biographies. Such sites pose little legal risk, though they need to be kept current, or consumers may be alienated by out-of-date information.

Another popular informational function is the publication of general medical or health information and literature. As long as this information is published for legitimate educational or entertainment value, publication is privileged under the First Amendment. The validity and currency of such materials should be disclaimed, and their provision for educational and entertainment rather than specific health care purposes stated. The most frequent method of publication is "linking" of the website to other sites containing articles or papers in electronic form. Such materials may be proprietary, and unauthorized linking may violate copyright laws or other proprietary rights. Lawsuits have been filed both for unauthorized linking, and for unauthorized copying of materials from one web site to another.

Some Internet service providers ("ISPs") and an increasing number of health organization websites are making "consumer health records" available. A "consumer health record" is not a medical record, strictly speaking, but generally consists of a personal web page containing information about the consumer's health, caregivers and the like, generally but not necessarily self-reported. Consumer health records of this type should not be considered a reliable basis for medical judgment, but should be kept secured against unauthorized access. Consumer health records should not be implemented without appropriate privacy and security features and disclosures, and disclaimers of their limited reliability and invalidity for clinical purposes.

One emerging function links consumer health records, or self-reported consumer health information, to medical literature search and indexing tools. Such a system might, for example, provide a consumer reporting asthma-like systems with up-to-date literature on asthma treatments. As long as the system retrieves generalized

information, such publication should remain privileged and permissible. In the event the system publishes personalized information including treatment recommendations, however, it is at risk of being deemed a "clinical expert system," which must be approved by the Food and Drug Administration prior to consumer use without professional supervision.

Office-to-Office and Peer-to-Peer E-mail. E-mail is probably unparalleled as a means of communicating administrative information, such as arranging hospital appointments. It can also be an extremely valuable tool for communications between busy practitioners, especially for non-emergency consultation or referral communications. Like access to on-line services, e-mail is readily available to anyone with a personal computer and Internet services provider.

But e-mail should not be adopted without some forethought about how it is used, including specifying who in the practice is responsible for what communications, making sure e-mail is checked routinely, keeping records of important communications, and specifying limitations on what can be communicated by e-mail. In particular, patient-identifiable information should not be communicated without encryption and access controls in place (see below). For most other content, however, no special technology is needed.

Physician-Patient E-Mail. Physician-patient e-mail has the potential to be both very valuable and very risky. It should not be adopted without careful analysis, specific written policies for its use and appropriate technologies and procedures to ensure it is kept private.

On the plus side, some practices in technologically sophisticated areas have seen real patient demand for e-mail, frequently from the most affluent sector, making it an attractive feature for "high end" practice. It has also proven valuable for communication with patients with chronic conditions for routine monitoring and counseling. On the negative side, it is highly risky (in some cases amounting to malpractice) to make diagnostic or treatment decisions based on e-mail communications, where the supporting information is limited to self-reported text statements (as opposed to in-person examination, where visual cues and physical testing is available). Patient expectations and physician uses of physician-patient e-mail therefore need to be carefully managed, probably including informed consent to its use for some clinically-related purposes.

Physician-patient e-mail also raises a genuine risk that confidential communications will be misdirected or intercepted by others. A patient's spouse might pick up her confidential e-mail at their joint home computer, for example, and e-mail sent to a patient at work in fact becomes the property of his employer (as the owner of the computer system), and therefore loses all confidentiality. More than that, existing regulations actually require encryption and authentication of the identities of the parties to e-mail containing some kinds of health care information, and emerging standards of care suggest it may be negligent not to use such practices. Physician-patient e-mail therefore needs to be carefully approached to ensure that appropriate security technologies and procedures are used and documented.

Practice Management Applications. Practice management programs can include a variety of scheduling, budgeting and claims management applications. These

can be very useful as long as they are actually integrated with the practice, so that they are used reliably and efficiently. Applications which are not used to communicate outside the organization present low privacy and security risks, but even patient billing information contained in such systems needs to be protected against improper disclosure. Only trained and authorized personnel should have access to sensitive data.

Electronic Medical Records. While electronic medical records hold promise, at this point there is no standard definition and the term "electronic medical record" may be applied (by their vendors, at least) to a wide range of applications. As with practice management applications, an electronic medical record system may be quite valuable if it is integrated with the practice.

Unfortunately, experience teaches that it may be difficult to integrate electronic medical record processes with physician practices. Computer terminals in examining rooms may be a distraction from patient interaction and in most cases are probably not cost-effective. A number of vendors are developing hand-held devices which may make electronic medical record use easier, but these are not well-established. Privacy and security controls for this kind of application are essential, since almost all information in them is likely to be confidential.

Electronic medical records are likely to become sufficiently valuable for many, perhaps most physician practices to acquire in the reasonably near future. However, these applications present the most significant practice integration issues, so the decision to use one should be based on a careful analysis of its intended uses and functions.

3. Due Diligence in ASP Selection.

It can be difficult to distinguish a "good" ASP, which fits a practice's needs, from "bad" ASPs which are difficult to integrate or do not perform as advertised. Unfortunately, it is necessary not only to identify "good" applications, it is also necessary to make sure they will be provided by "good" ASPs.

A "good" healthcare ASP is one which understands the environment in which its products will be used, has adapted its products accordingly, will support its integration into a practice, and will be around to back and upgrade its products for the long term. As with any major purchase, the best place to start in checking on a vendor is with references, preferably including existing users of the same applications. You should also check the vendor's financial backing, particularly if it is a startup or emerging company.

At least the following specific issues need to be addressed in qualifying a vendor of physician technology services:

Infrastructure and maintenance. Does the ASP have or can it provide the hardware, software, personnel and financial resources to install and maintain the application(s) over the life of the contract? Will the ASP provide appropriate training and "help desk" functions? What is included in the basic contract and what counts as an "upgrade?" Will the customer be required to upgrade, and will the ASP continue to support the basic product in case it issues an upgrade? What happens to the ASP's resources in case it is acquired or goes bankrupt? If a practice is going to become dependent on an application, it better have some assurance of continuity.

Privacy and security. How does the ASP propose to safeguard protected or other confidential information it may have access to? For example, an ASP providing electronic claims processing services will need to have comprehensive policies and procedures to ensure that the information it receives and systems it can access are very strongly protected. But even a vendor who is installing practice management software which will operate only in the practice will have to be allowed access to protected information for installation, troubleshooting and upgrade services. A physician practice which fails to obtain privacy and security assurances from such vendors will be liable for violating HIPAA. How does the ASP ensure the information is protected?

Suitable contract provisions. This is a problematic time for the drafting of contracts for HIT applications. The HIPAA privacy and security regulations will require specific, but unprecedented forms of agreement (called "business associate contracts" and/or "chain of trust agreements" – see Section 5, below, for details) among all parties to the exchange of protected health information. What form does the ASP use? Will they be appropriate under HIPAA? Do they realistically reflect the ASP's obligations and have suitable remedies for non-compliance? Information contracting can be a slippery thing, and it would be prudent to work with legal counsel who is experienced in this field.

Data Ownership. If the ASP has access to or hosts data for an application, who owns it? The ASP should not, but the law is far from clear and it needs to be explicitly agreed. Further, the ASP should disclose if it intends to create "anonymized" or "aggregated" secondary data sets derived from the practice's information, which may be a significant source of revenues for some ASPs. This practice is not illegal and is not

necessarily risky (though it may be), but there seems to be no reason why the ASP should have all the profit.

4. Privacy and Security Considerations.

One of the major emerging issues in the healthcare sector is compliance with the privacy and security regulations being issued by the Department of Health and Human Services ("HHS") under HIPAA. These regulations will impose a series of unprecedented requirements on physicians and all other caregivers and organizations in the health care sector, specifically directed at the management and protection of health care information. Compliance is likely to be mandatory as of some time in 2003, and failures to comply will lead to substantial civil or criminal penalties, may jeopardize accreditation, and could be grounds for private suits including class actions.

The regulations fall into two material categories:

- Security requirements requiring the adoption of comprehensive plans for the technological, administrative and legal protection of information systems used to store, process or transmit health information in electronic form; and

- Privacy standards stringently restricting the use or disclosure of health information, and requiring the adoption of a range of policies and procedures to ensure that these restrictions are not violated.

It is unlikely that HIT systems currently in use in most practices, and the policies and procedures in place for the use and protection of these systems and the information they contain will comply with these requirements. Bringing systems and

operations into compliance may be an expensive proposition for some practices, though it many of these concerns may be overstated.

Since HIT risk management is not a physician's primary mission and physician practices generally cannot afford a great depth of staff expertise in these matters, they already face challenges in making sure their own systems and processes are compliant. The burden of monitoring community standards for HIT compliance, assuring that systems are managed in a compliant fashion, and ensuring that users are properly trained for compliance would require a substantial organizational commitment for a physician organization.

By contrast, HIPAA compliance must be central to any healthcare ASP, since its business depends upon customers being satisfied that using it will not expose them to such risks. A specialized HIT ASP must develop and maintain expertise in HIPAA compliance to an extent which may otherwise be available only to very large health systems. While an ASP could not assume all compliance burdens, applicable security and privacy compliance standards and training should be integrated into almost any service packages it offered in the first place. An ASP with a credible, competent HIPAA compliance plan could therefore help a physician practice with HIPAA compliance, though it could not assume all the burdens.

5. Business Associate Agreements and ASPs.

Lawyers advising physicians should already be aware that privacy and security regulations being issued by the United States Department of Health and Human Services ("DHHS") pursuant to appear likely to dramatically change the way healthcare

information about individuals ("Protected Health Information") is managed. These regulations ("Privacy Standards" and "Security Standards" respectively) will apply to hospitals, physicians, health plans and the information services organizations which serve them ("Covered Entities"). At the time this article is being written it appears probable compliance will be required some time in mid-2003.

The Privacy and Security Standards will cover a number of important areas whose analysis is beyond this article. For lawyers in particular, however, one of the more problematic HIPAA compliance areas is likely to the drafting of appropriate contracts. Contracts are supposed to be our territory, and our clients may assume we have simple answers to literally unprecedented problems we will face in drafting such contracts. Worse yet, these contracts will have to be negotiated with a wide range of trading and operational partners, for a very wide range of purposes. If we are to avoid contract management nightmares in the future, we as a profession need to work together to develop consistent, though probably not uniform forms of contract.

Health care providers and related organizations cannot operate without disclosing Protected Health Information to each other and to other kinds of entities and individuals. Some disclosures are obvious, such as those for clinical referral and consultation, or claims submissions. Quality assurance, peer review and the like are also fairly apparent. But others are not so evident; what about information disclosed for financial audits? Closer to home, what about information disclosed to outside counsel? All of these relationships and many more require Covered Entities to disclose Protected Health Information for legitimate reasons. And virtually all such disclosures will have to be subject to new contracts whose forms we have yet to develop.

The draft Privacy and Security Standards each require that information exchanges be subject to some kind of contract between the exchanging parties. The Privacy Standards require a "Business Associate Contract," while the Security Standards require a "Chain of Trust Agreement." The distinction between the two types of contract is an artifact of the process by which the two sets of regulations were drafted, and it has been suggested that the two will be combined in the final versions, or at least consistent terminology will be used. By whatever name, crafting and negotiating these contracts will pose a challenge.

A Business Associate Contract is definable as an agreement whose terms follow and concern the treatment of Protected Health Information disclosed by a Covered Entity to virtually any other organization or individual ("Business Associate"). This form of contract primarily serves to indirectly bind Business Associates to the same obligations the Privacy Regulations impose directly on the disclosing Covered Entity.

A Chain of Trust Agreement, by contrast, follows and concerns the information systems and communications channels in which Protected Health Information is stored, processed and transferred. This kind of agreement is one element needed to create a "trust relationship" between systems operated by different organizations, which can allows users on each of the two systems to obtain or process information in the other system.

The Security Standards provide no details about the terms required for Chain of Trust Agreements, but generally speaking network "trust management" requires the implementation of policies and procedures which ensure that only properly qualified and

authorized users are permitted to have access to protected or sensitive systems or information. Since the terms under which users will be entitled to have access to Protected Health Information must be drawn from the Privacy Regulations, it seems reasonable to combine both types of agreement into one form.

Whatever the name, the parties to Business Associate/Chain of Trust Agreements will have to resolve at least the following issues, in addition to the usual difficult questions of indemnification, termination, etc. Any or all of these issues are likely to be present in contracting with an ASP:

- What kinds of Protected Health Information are subject to disclosure under the agreement?

- What uses may a party receiving Protected Health Information make of it? For example, a health care clearinghouse should be limited to processing and transmitting such information as required for claims submission.

- Are there any additional parties to which such information may be disclosed? It would be desirable to answer this question in both general and specific terms; for example, the health care clearinghouse in the foregoing example might be permitted to disclose information both to the specific, identified plans who pay the physician's claims for their enrollees, and in general to law enforcement agencies in response to appropriate process.

- What are the procedures by which a subject individual may seek to view, and/or request an amendment of or correction to information, if applicable?

- The party receiving information should warrant to the information source that it will not use or disclose any Protected Health Information received from the disclosing physician for any purpose outside the scope of services stated in its contract.

- Physicians who share or transmit information by network need to establish a set of security policies and procedures to establish "trusted systems" for the handling of all processes involving protected information. These security items include but are not necessarily limited to:

  - Commercially reasonable authentication processes for access to protected information by authorized individuals.

  - Hardware/software configuration which precludes unauthorized access to or disclosure of protected information. This analysis should include an assessment of possible weak points, and a description of the way the configuration is integrated with physical and corporate security items.

  - Physical security, ensuring that unauthorized personnel do not have access to sites or facilities which would permit them to view, process or disclose protected information.

  - Corporate security, including:

    - Designation of a senior officer or officers with responsibility for security oversight.

- Specifications and job descriptions for "trusted" positions (positions which are permitted access to protected information or sensitive systems, including the justification for such access)

- A prohibition against all non-trusted personnel having access to protected information or sensitive systems.

- Competent background check processes for qualification of trusted personnel.

- Disciplinary policies and procedures for enforcement of applicable personnel policies.

- Incident response policies and procedures.

- Appropriate insurance.

- Protected Health Information integrity protection and backup processes.

- If either of the parties relies upon third parties to provide material aspects of their services, that party needs to verify that these services also comply with the contractual obligations of security and privacy (to the extent applicable given the kind of service), and will be in place or can be readily substituted throughout the term of the contract.

  - The parties should strongly consider including provisions for audits of security and privacy practices by an independent third party at least annually, with a provision for additional audits in case of material security or privacy breach incidents.

- Any long-term contract will have to include mechanisms allowing for amendment to incorporate policies or procedures needed to address changes in the law and/or newly identified security threats, etc.

These are really only an outline of some of the issues which health care organizations will have to address in contracting for compliance under HIPAA. Clearly, given the range of parties which will have to be using this kind of documentation, material inconsistencies in their provisions will lead to difficulties in their management and interpretation. At the same time, it is highly unlikely that any single form can be satisfactory for the range of situations and relationships these contracts will have to cover.

This field will need serious attention from good lawyers who can articulate the needs of a range of clients and find common ground. We probably cannot achieve uniformity, but we need to develop consistency. If we don't impose it at the start, the courts will do it for us in the longer, and more expensive run.